CLAIMS:

1. A control system for use with an electronic gaming device, the control system comprising:

control means including:

digital processing means;

memory means;

storage means;

one or more sets of game information, each comprising program means and/or data means, each set of game information representing a component required by the processing means to run a game on the gaming device, and being stored in the storage means;

input/output means;

data authentication means to authenticate a set of game information stored in the storage means, the authentication means being arranged to operate under the control of any one of a plurality of sets of authentication rules and being arranged to receive one of the sets of authentication rules when authentication is initiated, and to use the received rules to perform the authentication;

the gaming device being operated by one of the program means when the respective program means is loaded in to the memory means;

means for receiving power; and

means for supplying power to the control system, the means for supplying power in electrical communication with the means for receiving power.

2. The control system as described in Claim 1, wherein the data authentication means is arranged to be initiated by an authorized third party instructor and to receive one of the sets of authentication rules from the authorized third party instructor when authentication is initiated.

3. The control system as described in Claim 1, wherein, as well as the data authentication means, a data validation means is provided to validate a set of game information every time the respective set of game information is loaded from the storage means to the memory means.

4. The control system as described in Claim 1, wherein, the data validation means includes CRC checking means to perform a CRC calculation on the set of gaming information and to compare a calculated CRC value with a CRC value stored with the respective set of game

information.

5. The control system as described in Claim 1, wherein each program means and each data means includes an identification means, such that each program means and each data means is uniquely identified.

6. The control system as described in Claim 5, wherein the control means further comprise a means for controlling one or more peripheral devices.

7. The control system as described in Claim 6, further comprising a second means for controlling one or more peripheral devices, the second means for controlling peripheral devices in communication with the control means.

8. The control system as described in Claim 6, wherein the first means for controlling peripheral devices is an Input/Output Control Board (IOCB).

9. The control system as described in Claim 8, further comprising a non-volatile memory as the storage means.

10. The control system as described in Claim 9, wherein the storage means is chosen from the group consisting of a ROM, PROM, EPROM or EEPROM.

11. The control system as described in Claim 10, wherein the verification method further includes a method for grouping the program means that are related, and for grouping the data means that are related, the method for grouping emulating a method of grouping employed in storage media.

12. The control system as described in Claim 11, wherein the storage media whose grouping method is emulated is chosen from the group of storage media consisting of ROM, PROM, EPROM or EEPROM.

13. The control system as described in Claim 12, wherein the verification method further includes a method of abstracting the location of the program means, the data means and the storage means.

14. The control system as described in Claim 13, wherein the verification means further includes means to compare the identification means of the requested program means or of the requested data means to the established identification means.

15. The control system as described in Claim 14, wherein the verification means further includes a means for of controlling the operation of the gaming device in response to the verification of integrity of the program means or the data means.

16. The control system as described in Claim 15, wherein the means for controlling includes a means of halting the verification means if the identification means of the requested program means or the requested data means does not match the established identification means of the program means or the data means.

17. The control system as described in Claim 10, wherein the verification means further includes a means to authenticate the retrieved program means or the retrieved data means.

18. The control system as described in Claim 17, wherein the control means effects the means to authenticate only after the integrity of the requested program means or the integrity of the requested data means has been verified.

19. The control system as described in Claim 1, wherein the verification means for verifying the integrity of the program means and the data means further includes means to authentication means, for authenticating the program means and the data means, the authentication means being activated in response to signals received from a requesting means.

20. The control system as described in Claim 18, wherein the requesting means is an authentication agent.

21. The control system as described in Claim 16, wherein the authentication agent is external to the control system and the gaming device, the authentication agent being in communication with the control means.

22. The control system as described in Claim 16, wherein an authentication agent is external to the control system and is within the gaming device, the authentication agent being in communication with the control means.

23. The control system as described in Claim 17 or Claim 18, wherein the authentication method further includes a method for registering the authentication agents.

24. The control system as described in Claim 18, wherein the signal received from the requesting means is an authentication request.

25. The control system as described in Claim 1, wherein the control means further includes a means for receiving the authentication requests.

26. The control system as described in Claim 1, wherein the authentication requests includes a signal to prioritize the authentication request.

27. The control system as described in Claim 23, wherein the control means further includes a means of queueing the authentication requests, when more than one authentication request has been sent from the authentication agents.

28. The control system as described in Claim 24, wherein the control means further include a means of interpreting the authentication request.

29. The control system as described in Claim 25, wherein the means of interpreting the authentication request includes a means of generating an authentication identification (id) of the requested program means or data means.

30. The control system as described in Claim 26, wherein the control system further includes a responder means, the responder means being external to the control means and in electronic communication with the control means.

31. The control system as described in Claim 27, wherein the control means further includes a presenter means, the presenter means communicating the generated authentication id to the responder means.

32. The control system as described in Claim 28, wherein the control means and the responder means include a means for determining if the generated authentication id is authentic, the responder means comparing the generated authentication id to the request, the generated authentication id deemed authentic if the generated authentication id matches the request.

33. The control system as described in Claim 32, wherein the generated authentication id is deemed not authentic if the generated authentication id does not match the request.

34. The control system as described in Claim 22 and 33, wherein the control means further includes a means of controlling the operation of the gaming device in response to the determination of authenticity of the requested program means or the requested data means.

35. The control system as described in Claim 34, wherein the controlling means includes means of halting the operation of the gaming device if the requested program means or the requested data means is deemed not authentic.

36. The control system as described in Claim 34, wherein the controlling means includes means of continuing the operation of the gaming device if the requested program means or the requested data means is deemed

PCT/AU99/00486
Received 30 June 2000

authentic.

37. The control system as described in Claim 12, wherein the storage means is a hard disk drive unit.

38. The control system as described in Claim 12, wherein the storage means is a CD-ROM unit.

39. The control system as described in Claim 12, wherein the storage means is a DVD unit.

40. The control system as described in Claim 12, wherein the storage means is a file server.

41. For use in an electronic gaming device, a method to verify the integrity of program means and the integrity of data means stored in a control system, the control system comprising:

control means in electronic communication with the gaming device, the control means including;

digital processing means ;

memory means;

storage means;

one or more sets of game information, each comprising program means and/or data means, each set of game information representing a component required by the processing means to run a game on the gaming device, and being stored in the storage means;

input/output means;

means for receiving power; and

means for supplying power to the control system, the means for supplying power in electrical communication with the means for receiving power, the verification method comprising the steps of:

sending a request from a requesting means to the control system;

processing the request within the control system;

retrieving a requested program means or a requested data means from the storage means;

verifying the integrity of the requested program means or the requested data means by verification means which verify by comparing the identification means of the requested program means or the requested data means with the request, the integrity verified if the identification means matches the established identification means request; and

controlling the operation of the gaming device in response to the

verification of integrity of the requested program means or the requested data means.

42. The method as described in Claim 41, further comprising the steps of halting the verification method of the identification means if the requested program means or the requested data means does not match the established identification means of the program means or the data means.

43. The method as described in Claim 42, further comprising a method to authenticate the retrieved program means or the retrieved data means.

44. The method as described in Claim 43, wherein the method to authenticate is effected only after the integrity of the requested program means or the integrity of the requested data means has been verified.

45. The method as described in Claim 44, wherein the requesting means is an authentication agent.

46. The method as described in Claim 43, wherein the method further includes a method for registering the authentication agent.

47. The method as described in Claim 46. wherein the request includes a verification request and an authentication request.

48. The method as described in Claim 47, wherein the request further includes an authentication queuing request.

49. The method as described in Claim 48, wherein the request further includes registration means for the authentication agent.

50. The method as described in Claim 46, further including a method of abstracting the location of the program means, the data means, and the storage means.

51. The method as described in Claim 50, further including the step determining which of the program means are related, and determining which of the data means are related.

52. The method as described in Claim 51, further including the step of grouping the related program means, and grouping the related data means.

53. The method as described in Claim 52, wherein the grouping step emulates a method of grouping employed in storage media chosen from the group consisting of ROM, PROM, EPROM or EEPROM.

54. The authentication method as described in Claim 53, wherein the control means further includes a means for queuing the authentication requests.

55. The authentication method as described in Claim 54, further

PCT/AU99/00486
Received 30 June 2000

comprising the step of queuing the authentication requests, when more than one authentication request has been sent from the authentication agents.

56. The authentication method as described in Claim 49, wherein the control means further includes a means of interpreting the authentication request.

57. The authentication method as described in Claim 56, further comprising the step of interpreting the authentication request.

58. The authentication method as described in Claim 57, wherein the interpretation step includes the step of generating an authentication identification (id).

59. The authentication method as described in Claim 58, wherein the control means further includes a presenter means, the presenter means communicating the generated authentication id to a responder means.

60. The authenticating method as described in Claim 59, further comprising the step of determining if the generated authentication id is authentic, the responder means and the control means comparing the generated authentication id to the request, the generated authentication id deemed authentic if the generated authentication id matches the request.

61. The authentication method as described in Claim 60, wherein the generated authentication id is deemed not authentic if the generated authentication id does not match the request.

62. The authentication method as described in Claim 60 or 61, further including the step of controlling the operation of the gaming device in response to the determination of authenticity of the requested program means or the requested data means.

63. The method as described in Claim 62, wherein the controlling step includes halting the operation of the gaming device if the requested program means or the requested data means is determined to be not authentic.

64. The method as described in Claim 62, wherein the controlling step includes continuing the operation of the gaming device if the requested program means or the requested data means is determined to be authentic.